REMARKS

I. Introduction

In response to the Office Action dated July 24, 2006, claims 1, 10, 19, and 28 have been amended. Claims 1-36 remain in the application. Re-examination and re-consideration of the application, as amended, is requested.

II. Prior Art Rejections

In paragraph (5) of the Office Action, claims 1, 2, 4, 5, and 8 were rejected under 35 U.S.C. §103(a) as being unpatentable over Cohen et al., U.S. Patent No. 5,282,249 (Cohen) in view of Kocher et al., U.S. Patent No. 6,289,455 (Kocher) and further in view of Wong et al., U.S. Patent No. 6,278,633 (Wong). In paragraph (11) of the Office Action, claims 3, 6, and 7 were rejected under 35 U.S.C. §103(a) as being unpatentable over Cohen in view of Kocher, in view of Wong, and further in view of Pitts, U.S. Publication No. 20020145931 (Pitts). In paragraph (15) of the Office Action, claim 9 was rejected under 35 U.S.C. §103(a) as being unpatentable over Cohen in view of Kocher, in view of Wong, and further in view of Barth, U.S. Patent No. 6,334,216 (Barth). In paragraph (17) of the Office Action, claims 10, 11, 13, 14, 17, 18, 27-29, 31, 32, and 35-36 were rejected under 35 U.S.C. §103(a) as being unpatentable over Kocher in view of Barth and further in view of Wong. In paragraph (31) of the Office Action, claims 12, 15, 16, 30, 33, and 34 were rejected under 35 U.S.C. §103(a) as being unpatentable over Kocher in view of Barth in view of Wong and further in view of Pitts. In paragraph (38) of the Office Action, claims 19, 20, 22, 23, and 26 were rejected under 35 U.S.C. §103(a) as being anticipated by Kocher in view of Wong. In paragraph (44) of the Office Action, claims 21, 24, and 25 were rejected under 35 U.S.C. §103(a) as being unpatentable over Kocher in view of Wong and further in view of Pitts.

Applicants respectfully traverse these rejections.

Specifically, the independent claims were rejected as follows:

> As per claim 1, Cohen discloses a system for controlling access to digital services comprising:
>
> (a) A control center configured to coordinate and provide digital services (see Fig. 2);
>
> (b) An uplink center configured to receive the digital services from the control center and transmit the digital services to a satellite (see Fig. 1/1 #20);
>
> (c) The satellite configured to:
>
> Receive the digital services from the uplink center (Fig. 1/1 #22);

Process the digital services (Fig. ½ #22 wherein processing of digital services is the intrinsic step that allows transmission); and

Transmit the digital services to a subscriber receiver station (Fig. 1/2 #24);

(d) The subscriber receiver station configured to:

Receive the digital services from the satellite (Fig. 1/2 #26);

Control access to the digital services through an integrated receiver/decoder (IRD) (Fig. 1/2 #30);

(e) A conditional access module (CAM) communicatively coupled to the IRD (Fig. 1/2 #32);

but does not disclose wherein the CAM comprises:

a protected nonvolatile memory component, wherein:

the protected nonvolatile memory component is used to contain state information to provide desired functionality and enforce one or more security policies for accessing the digital services; and

the protected nonvolatile memory component is protected from modification such that the protected nonvolatile memory component is read only;

access to the protected nonvolatile memory component is isolated;

a microprocessor's unprotected nonvolatile memory component wherein programming control and a programming charge pump are shared by both the protected nonvolatile memory component and the microprocessor's un-protected nonvolatile memory component;

a hidden non-modifiable identification number embedded into the protected nonvolatile memory component, wherein the identification number uniquely identifies the CAM; and

the identification number is used to limit a cloning attack wherein said cloning attack comprises copying the identification number to a new CAM; and

a fixed state custom logic block, wherein the protected nonvolatile memory component is not directly accessible via a system bus and access to the protected nonvolatile memory component is limited to the custom logic block.

Kocher discloses wherein the CAM (Fig. 2 #225 wherein the CAM is the cryptographic rights unit) comprises:

a protected nonvolatile memory component (column 21 lines 13-15), wherein:

the protected nonvolatile memory component is used to contain state information to provide desired functionality and enforce one or more security policies for accessing the digital services (column 10 lines 36-38 and 43-47 wherein the digital services is pay-tv); and

the protected nonvolatile memory component is protected from modification such that the protected nonvolatile memory component is read only (column 10 lines 43-47);

and

access to the protected nonvolatile memory component is isolated (Fig. 2 #265);

a hidden non-modifiable identification number embedded into the protected nonvolatile memory component, wherein the identification number uniquely identifies the CAM (column 7 lines 65-67 column 10 lines 38-40 and 43-45: it can be

understood that the device key necessarily applies to an identification number which as used by the applicant is a security-related parameter. Moreover, in view of column 10 lines 61-65 and column 11 lines 53-65 it can clearly be seen that the rights key which is generated from the device key/identification number is used to decrypt/access the content; which meets the functionality of the identification number as defined by the Applicant. Moreover in column 12 lines 24-32, 37-40 and 62-66, Kocher explains the use of the device key to determine permission of access to the services, which also meets a requirement of the identification number as stated by the Applicant); and

the identification number is used to limit a cloning attack wherein said cloning attack comprises copying the identification number to a new CAM (column 14 lines 2-9 and column 18 lines 37-45 and column 26 lines 25-40; It can be clearly seen that the function of the device key which is unique to a device implies a necessary concern that this key is not copied to another CAM. These passages clearly demonstrate that a compromised device key would require the cessation of enabling access to those CRUs containing that particular key. This is necessarily related to the cloning attack as discussed by the Applicant wherein if an identification number is known to be used by multiple devices illegally, those devices using that number would not longer be effective); and

a fixed state custom logic block, wherein the protected nonvolatile memory component is not directly accessible via a system bus and access to the nonvolatile memory component is limited ot the custom logic block (Fig. 2 #260 wherein the CryptoFirewall is the custom logic block).

Kocher is analagous art because it discussed a method and apparatus for preventing piracy of digital content including the use of a smart card.

It would have been obvious at the time of the invention to include the features of the CAM found in Kocher in the smart card used by Cohen to control access to the broadcasted data.

Motivation for one to modify Cohen as discussed above would have been to improve the security of systems used to distribute and protect digital content (from piracy or attackers) as taught in Kocher (column 5 lines 55-56).

Kocher does not disclose a microprocessor's unprotected nonvolatile memory component wherein programming control and a programming charge pump are shared by both the protected nonvolatile memory component and the microprocessor's unprotected nonvolatile memory component;

Wong does disclose wherein programming control and a programming charge pump is shared by memory (column 3 lines 7-19 and column 4 lines 1-7).

Wong is analagous art because it is directed to system concerning the use of non-volatile memory in a circuit.

It would have been obvious to modify Kocher to include wherein the various memory units, protected and unprotected, share programming control and a programming charge pump. Kocher discussed that the protected and unprotected memory are located on the same chip, thus enabling the use of a common programming control and charge pump.

Motivation for one to modify Kocher as discussed above would have been obvious to one of ordinary skill in the art. As discussed and implied in Wong,

sharing a charge pump provides uniformity for a read or write voltage used when accessing the memory cells (column 3 lines 10-13). One of ordinary skill in the art should understand that the practice of sharing a charge pump is very common in the circuit design and practice and thus motivation for modifying Kocher would include the inherent advantages of sharing charge pumps as is known in the art.

As per claim 10, Kocher discloses a method for limited unauthorized access to digital services comprising:

Embedding a hidden non-modifiable identification number into a protected nonvolatile memory component (column 21 lines 13-15 and column 18 lines 37-45 wherein the identification number is the serial number alluded to and which is stored in the protected memory and is non-modifiable in the same manner as the unique BATCH_KEY described in column 18 lines 49-52; see also claim 1), wherein:

The protected nonvolatile memory component is used to contain state information to provide desired functionality and enforce one or more security policies for accessing the digital services (column 10 lines 36-38 and 43-47 wherein the digital services is pay-tv);

The hidden non-modifiable identification number uniquely identifies a device containing the protected nonvolatile memory component (column 18 lines 37-45 see also claim 1); and

the identification number is used to limit a cloning attack wherein said cloning attack comprises copying the identification number to a new CAM (column 14 lines 2-9 and column 18 lines 37-45 and column 26 lines 25-40; It can be clearly seen that the function of the device key which is unique to a device implies a necessary concern that this key is not copies to another CAM. These passages clearly demonstrate that a compromised device key would require the cessation of enabling access to those CRUs containing that particular key. This is necessarily related to the cloning attack as discussed by the Applicant wherein if an identification number is known to be used by multiple devices illegally, those devices using that number would no longer be effective); and

Isolating access to the nonvolatile memory component such that access to the nonvolatile memory component is limited to a fixed state custom logic block (Fig. 2 #260 wherein the CryptoFirewall is the custom logic block as described in column 21 lines 34-35), the nonvolatile memory component is protected such that the nonvolatile memory component is read only (column 10 lines 43-47), and the nonvolatile memory component is not direclty accessible via a system bus (Fig. 2 #260).

But does not disclose wherein access to the digital services is based on access rights associated with the hidden non-modifiable identification number and programming control and a programming charge pump are shared by both the protected nonvolatile memory component and a microprocessor's unprotected nonvolatile memory component.

Barth does disclose wherein access to the digital services is based on access rights associated with an identification number (column 4 lines 33-45 wherein the access rights is whether it is associated with a blocking note).

Barth is analagous art because it discloses a method of gaining access to services based on an identification number utilized in an access card.

It would have been obvious for one of ordinary skill in the art at the time of the invention to modify Kocher to include the method of comparing an identification number to a list of unauthorized numbers and their access rights before granting access.

Motivation for one to modify Kocher as discussed above would have been to allow system management to prevent access to the services if the corresponding number is reported as lost or if the user is delinquent in his obligations for the services offered as taught in Barth (column 3 lines 37-42).

Wong does disclose wherein programming control and a programming charge pump is shared by memory (column 3 lines 7-19 and column 4 lines 1-7).

Wong is analagous art because it is directed to system concerning the use of non-volatile memory in a circuit.

It would have been obvious to modify Kocher to include wherein the various memory units, protected and unprotected, share programming control and a programming charge pump. Kocher discussed that the protected and unprotected memory are located on the same chip, thus enabling the use of a common programming control and charge pump.

Motivation for one to modify Kocher as discussed above would have been obvious to one of ordinary skill in the art. As discussed and implied in Wong, sharing a charge pump provides uniformity for a read or write voltage used when accessing the memory cells (column 3 lines 10-13). One of ordinary skill in the art should understand that the practice of sharing a charge pump is very common in the circuit design and practice and thus motivation for modifying Kocher would include the inherent advantages of sharing charge pumps as is known in the art.

As per claim 19, Kocher discloses a conditional access module (CAM), (Fig. 2 #225 wherein the CAM is the cryptographic rights unit) comprising:

A microprocessor (column 21 lines 1-5);

An unprotected nonvolatile memory component connected to the microprocessor (column 21 lines 1-5);

a protected nonvolatile memory component (column 21 lines 13-15), wherein:

the protected nonvolatile memory component is used to contain state information to provide desired functionality and enforce one or more security policies for accessing the digital services (column 10 liens 36-38 and 43-47 wherein the digital services is pay-tv); and

the protected nonvolatile memory component is protected from modification such that the protected nonvolatile memory component is read only (column 10 lines 43-47);

and

access to the protected nonvolatile memory component is isolated (Fig. 2 #265);

a hidden non-modifiable identification number embedded into the protected nonvolatile memory component, wherein the identification number uniquely

identifies the CAM (column 7 lines 65-67 column 10 lines 38-40 and 43-45: it can be understood that the device key necessarily applies to an identification number which as used by the applicant is a security-related parameter. Moreover, in view of column 10 lines 61-65 and column 11 lines 53-65 it can clearly be seen that the rights key which is generated from the device key/identification number is used to decrypt/access the content; which meets the functionality of the identification number as defined by the Applicant. Moreover in column 12 lines 24-32, 37-40 and 62-66, Kocher explains the use of the device key to determine permission of access to the services, which also meets a requirement of the identification number as stated by the Applicant); and

the identification number is used to limit a cloning attack wherein said cloning attack comprises copying the identification number to a new CAM (column 14 lines 2-9 and column 18 lines 37-45 and column 26 lines 25-40; It can be clearly seen that the function of the device key which is unique to a device implies a necessary concern that this key is not copied to another CAM. These passages clearly demonstrate that a compromised device key would require the cessation of enabling access to those CRUs containing that particular key. This is necessarily related to the cloning attack as discussed by the Applicant wherein if an identification number is known to be used by multiple devices illegally, those devices using that number would no longer be effective);

and

a fixed state custom logic block, wherein the protected nonvolatile memory component is not directly accessible via a system bus and access to the protected nonvolatile memory component is limited to the custom logic block (Fig. 2 #260 wherein the CryptoFirewall is the custom logic block).

Kocher does not disclose the CAM wherein programming control and a programming charge pump are shared by both the protected nonvolatile memory component and the un-protected nonvolatile memory component.

Wong does disclose wherein programming control and a programming charge pump is shared by memory (column 3 lines 7-19 and column 4 lines 1-7).

Wong is analagous art because it is directed to system concerning the use of non-volatile memory in a circuit.

It would have been obvious to modify Kocher to include wherein the various memory units, protected and unproteced, share programming control and a programming charge pump. Kocher discussed that the protected and unprotected memory are located on the same chip, thus enabling the use of a common programming control and charge pump.

Motivation for one to modify Kocher as discussed above would have een obvious to one of ordinary skill in the art. As discussed and implied in Wong, sharing a charge pump provides uniformity for a read or write voltage used when accessing the memory cells (column 3 lines 10-13). One of ordinary skill in the art should understand that the practice of sharing a charge pump is very common in the circuit design and practice and thus motivation for modifying Kocher would include the inherent advantages of sharing charge pumps as is known in the art.

Claim 28 is rejected because it discussed the same subject matter as claim 10.

Independent claims 1, 10, 19 and 28 are generally directed to the use of an identification number. Specifically, the claims address an identification number that is used to limit a cloning attack. As set forth throughout the specification (including paragraphs [0062], [0072]-[0074], and [0078]), the identification number uniquely identifies the device (i.e., the CAM) and such an identifier is used in a particular context. In this regard, the claims specifically provide that the identification number is used to limit a cloning attack wherein such a cloning attack comprises copying the identification number to a new pirated CAM. As indicated in the specification, hacking techniques typically use a low cost cloning attack wherein the identity of a pirate card is copied to a new card. The claims provide for hiding this identification number in the isolated nonvolatile memory component. By preventing access to the identification number (except through the custom logic block), the low cost cloning attack techniques are limited.

In addition, Applicants note that the claims provide further limitations. Namely, the claims provide for two nonvolatile memory components. One nonvolatile memory component is protected and contains the hidden number as described above. The other nonvolatile memory component is unprotected and is referred to as a microprocessor's unprotected nonvolatile memory component. The claims provide specific limitations and details regarding both the protected and unprotected nonvolatile memory components. In this regard, the claims provide that programming control and a programming charge pump are shared by both nonvolatile memory components. In addition, the amended claims now provide that the data and address lines of the protected nonvolatile memory component are routed only to the fixed state custom logic block Thus, not only do the two different nonvolatile memory components share programming control and a charge pump, but the data and address lines of the protected component are routed only to the fixed state custom logic block.

Neither of the cited references teach nor suggest these various elements of Applicants' independent claims. The Office Action relies on Kocher to teach the protected nonvolatile memory component. However, nowhere in Kocher is there any discussion of the unique configuration wherein there are multiple nonvolatile memory components that not only share programming control and a charge pump but also wherein data and address lines of the protected component are only routed to the fixed state custom logic block.

The Office Action admits that Kocher fails to teach the shared programming control and charge pump and instead relies on Wong for such an aspect. Applicants note that Wong actually requires a pipelined memory access (see col. 3, lines 7-19). Such a pipeline would clearly teach away from the present invention wherein one component is protected and one is not protected such that the two components do not share data and address lines. Since the amended claims require the data and address lines routed only to the fixed state custom logic block, and the other component is not-protected (i.e., and not routed to the custom logic block), Wong cannot possibly teach the shared charge pump between the two nonvolatile memory components. Again, Wong would require the pipelined memory wherein the data and address lines are required to be shared between the memory cells. In this regard, Wong teaches away from the present invention. Consequently, as presently set forth in the amended claims, the combination of Wong with Kocker (and/or Cohen) would not produce the claimed invention.

Moreover, the various elements of Applicants' claimed invention together provide operational advantages over Cohen, Kocher, Wong, Pitts, and Barth. In addition, Applicants' invention solves problems not recognized by Cohen, Kocher, Wong, Pitts, and Barth

Thus, Applicants submit that independent claims 1, 10, 19, and 28 are allowable over Cohen, Kocher, Wong, Pitts, and Barth. Further, dependent claims 2-9, 11-18, 20-27, and 29-36 are submitted to be allowable over 1, 10, 19, and 28, respectively, and thus contain all the limitations of the independent claims. In addition, dependent claims 2-9, 11-18, 20-27, and 29-36 recite additional novel elements not shown by Cohen, Kocher, Wong, Pitts, and Barth.

III. Conclusion

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited. Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Respectfully submitted,

By: _____
Name: Georgann S. Grunebach
Reg. No.: 33,179

Date: October 24, 2006

The DIRECTV Group, Inc.
CA/LA1/A109
2230 E. Imperial Highway
P. O. Box 956
El Segundo CA 90245

Telephone No. (310) 964-4615